UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

RITA MAY AND TAMMIE CREEK, individually, and on behalf of all other similarly situated, Plaintiffs, vs. APRIA HEALTHCARE LLC, Defendant.	CASE NO. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Rita May and Tammie Creek ("Plaintiffs"), by and through their attorneys of record, upon personal knowledge as to their own acts and experiences, and upon information and belief as to all other matters, files this complaint against Apria Healthcare LLC ("Apria" or "Defendant") and alleges the following:

INTRODUCTION

1. Plaintiffs bring this class action complaint on behalf of a class of persons impacted by Defendant's failure to safeguard, monitor, maintain and protect highly sensitive Personal Health Information ("PHI") and Personally Identifiable Information ("PII") (collectively "Sensitive Information"). Defendant collected, stored, and maintained its patients', including Plaintiffs' and the Class's, Sensitive Information as part of its home healthcare equipment services, which Defendant provides nationwide.

2. On September 1, 2021, Apria learned that its networks containing its patients' Sensitive Information were impacted during a cyberattack ("Data Breach"). Specifically, Defendant received a notice that certain Apria systems were accessed by hackers who, subsequently, gained access to patients' Sensitive Information. Defendant disclosed that its Data

Breach exposed Sensitive Information including Plaintiffs' and the Class Members' personal, medical, health insurance, and financial information, and social security numbers.

3. Although Defendant discovered the Data Breach on September 1, 2021, it inexplicably waited until May 24, 2023, twenty months later, to issue a public notice of its data breach and purportedly to begin issuing direct notice to the patients impacted by the Data Breach. In its online Data Breach notice, Apria admitted that Defendant's networks and systems had been breached and that the cyberattack exposed highly sensitive information.

4. The Data Breach impacted the sensitive personal information of approximately 1,049,375 individuals.

5. The type of information impacted by the Data Breach can be used to orchestrate a host of fraudulent activities, including medical, insurance, and financial fraud and identity theft. Indeed, the entire purpose of these types of medical data breaches is to misuse the stolen information or to sell it to fraudsters on the dark web. Consequently, all impacted individuals are at a heightened and significant risk that their information will be disclosed to criminals and misused for attempted or actual fraud or identity theft.

6. As a result of Defendant's lax data security concerning its systems and servers, nearly 2 million of Defendant's patients have had sensitive details of their lives and identities accessed, viewed and stolen by malicious cybercriminals. These patients have been placed in an immediate and continuing risk of harm from fraud, identity theft, and related harm caused by the Data Breach.

7. Defendant's conduct, consequently, required Plaintiffs and the Class to have to undertake time-consuming, and often costly, efforts to mitigate the actual and potential harm caused by the Data Breach's exposure of their Sensitive Information, including by, among other

things, placing freezes and alerts with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, reviewing and monitoring their credit reports and accounts for unauthorized activity, changing passwords on potentially impacted websites and applications, and requesting and maintaining accurate medical records. Minors, additionally, may not be able to monitor the impact of the Data Breach on their lives for years, at which point the damage will be done.

8. As such, Plaintiffs and the Class bring this action to recover for the harm they suffered, and assert the following claims: negligence, negligence per se, and breach of implied contract.

JURISDICTION AND VENUE

9. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiffs and at least one member of the putative Class, as defined below, are citizens of a different state than Defendant Apria, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

10. This Court has general personal jurisdiction over Defendant Apria because Apria maintains its principal place of business in Indianapolis, Indiana, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Apria's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

12. **Plaintiff** Rita May is a resident and citizen of Richmond, Missouri. She received medical services from Apria, including purchasing CPAP supplies. Plaintiff provided Apria with her sensitive PII and PHI for purposes of receiving her medical equipment and/or services. Upon information and belief, her information was part of Apria's Data Breach, she was sent a Data Breach Notice, and as a result of the Data Breach, her information is in the hands of criminals.

13. **Plaintiff** Tammie Creek is a resident and citizen of Little Rock, Arkansas. She received medical services from Apria. Plaintiff provided Apria with her sensitive PII and PHI for purposes of receiving her medical equipment and/or services. Upon information and belief, her information was part of Apria's Data Breach, she was sent a Data Breach Notice, and as a result of the Data Breach, her information is in the hands of criminals.

14. **Defendant** Apria Healthcare LLC is a Delaware company that operates its principal place of business at 7553 Company Drive, Indianapolis, Indiana, 46237.

FACTUAL BACKGROUND

A. Defendant Collected, Maintained and Stored Sensitive Information.

15. Apria purports to be a leading provider of home healthcare equipment and related services across the USA. It provides equipment related to home respiratory therapy, sleep therapy, pharmacy networks, negative pressure wound therapy, and other home medical equipment.[1]

16. Defendant is an experienced and sizeable company and boasts of having served 2.05 million patients in 2021 alone, and of having 275 branches with 6,500 team members.[2]

17. As an ordinary and regular part of the services that it provides to its patients, Defendant collects, creates, and maintains personal patient information. Defendant's Notice of

[1] https://www.apria.com/about-us

[2] https://www.apria.com/

Data Breach, posted online, claims that "Apria takes the safeguarding of personal information seriously and regrets any concern this may cause."[3]

18. The personal and medical information that Defendant maintains is highly sensitive. To obtain healthcare services, patients, like Plaintiffs and the Class, must provide Defendant with their medical providers with highly sensitive information, including PHI, PII, or both. As a massive healthcare service provider, Defendant has collected and maintained a sizeable depository of Sensitive Information, acting as a particularly lucrative target for data thieves looking to obtain and misuse or sell patient data.

19. Plaintiffs and the Class had a reasonable expectation that Defendant would protect the Sensitive Information that it collected and maintained, especially because, given the publicity of other data breaches and the significant impact they had, Defendant knew or should have known that failing to adequately protect their information could cause substantial harm.

20. Defendant's Privacy Policy acknowledges the sensitivity of the information that it maintains, along with the legal requirements for Defendant to confidentially maintain such information. In particular, Defendant's Privacy Policy that it uses "reasonable security measures to protect the Personally identifiable Information [it] collect[s] and store[s] form loss, misuse, destruction, or unauthorized access."[4] It also purports to comply with HIPAA.[5]

21. As described throughout this Complaint, Defendant did not reasonably protect, secure, or store Plaintiffs' and the Class's Sensitive Information prior to, during, or after the Data Breach, but rather enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Defendant maintained.

---

[3] https://www.apria.com/notice-of-data-breach

[4] https://www.apria.com/privacy-policy

[5] *Id.*

Consequently, cybercriminals circumvented Defendant's security measures, resulting in a significant data breach.

B. Defendant Suffered a Massive Data Breach Exposing Patients' Sensitive Information.

22. On September 1, 2021, Apria discovered suspicious activity on its systems. Apria claims to have initiated an investigation and taken containment measures at that point, but those measures were clearly insufficient. Apria later admitted that third-party hackers had gained access to its systems and gained access to highly sensitive PII, PHI, and financial information. Upon information and belief, during the Data Breach the hackers copied and exfiltrated substantial amounts of Plaintiffs' and the Class's Sensitive Information.

23. Defendant has purported to have sent out notices to the individuals impacted by the Data Breach, but they have not yet been received.

24. Apria waited more than a year and a half to issues its online notice and to start providing notice to the individuals impacted by the Data Breach. Specifically, despite identifying the Data Breach on September 1, 2021, it did not make the Data Breach public until May 24, 2023, 20 months later. A 20-month delay is patently unreasonable and put Plaintiffs and the Class at a continued and significant risk of harm that their stolen data, capable of being used for medical, insurance, or financial fraud and identity theft, would be misused. Had Defendant provided notice sooner, Class members would have been able to take mitigatory steps sooner.

25. Given that Defendant was storing the Sensitive Information of Plaintiffs and the Class and knew or should have known of the serious risk and harm caused by a data breach, Defendant was obligated to implement reasonable measures to prevent and detect cyber-attacks, such as those recommended by the Federal Trade Commission, required by the Health Insurance Portability and Accountability Act, and promoted by data security experts and other agencies. That

obligation stems from the foreseeable risk of a Data Breach given that Defendant collected, stored, and had access to a swath of highly sensitive patient records and data and, additionally, because other highly publicized data breaches at numerous healthcare institutions and a recent ransomware attack on Defendant put Defendant on notice that the higher personal data they stored might be targeted by cybercriminals.

26. Despite the highly sensitive nature of the information Defendant obtained, maintained, and stored, Defendant's recent ransomware attack, and the prevalence of health care data breaches, Defendant inexplicably failed to take appropriate steps to safeguard the Sensitive Information of Plaintiffs and the Class from being compromised. The Data Breach itself, and information Defendant has disclosed about the breach to date, including its length, the need to remediate Defendant's cybersecurity, the number of people impacted, and the sensitive nature of the impacted data collectively demonstrate Defendant failed to implement reasonable measures to prevent cyber-attacks and the exposure of the Sensitive Information it oversaw.

C. Exposure of Sensitive Information Creates a Substantial Risk of Harm.

27. The personal, health, and financial information of Plaintiffs and the Class is valuable and has become a highly desirable commodity to data thieves.

28. Defendant's failure to reasonably safeguard Plaintiffs' and the Class's Sensitive Information has created a serious risk to Plaintiffs and the Class, including both a short-term and long-term risk of identity theft.

29. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

30. According to experts, one out of four data breach notification recipients becomes a victim of identity fraud.[6]

31. Stolen Sensitive Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines and is frequented by criminals, fraudsters, and other wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal identities and online activity.

32. Moreover, according to Robert P. Chappell, Jr., a law enforcement professional, fraudsters can steal and use a minor's information until the minor turns eighteen years old before the minor even realizes he or she has been the victim of an identity theft crime.[7]

33. The risk to minor Class members is substantial given their age and lack of established credit. The information can be used to create a "clean slate identity," and use that identity for obtaining government benefits, fraudulent tax refunds, and other scams. There is evidence that children are 51% more likely to be victims of identity theft than adults.[8]

34. Purchasers of Sensitive Information use it to gain access to the victim's bank accounts, social media, credit cards, and tax details. This can result in the discovery and release of additional Sensitive Information from the victim, as well as Sensitive Information from family, friends, and colleagues of the original victim. Victims of identity theft can also suffer emotional distress, blackmail, or other forms of harassment in person or online. Losses encompass financial data and tangible money, along with unreported emotional harm.

---

[6] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims,* ThreatPost.com (last visited Jan. 17, 2022), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/

[7] Brett Singer, *What is Child Identity Theft?*, Parents (last visited Jan. 17, 2022), https://www.parents.com/kids/safety/tips/what-is-child-dentity-theft/.

[8] Avery Wolfe, *How Data Breaches Affect Children*, Axion Cyber Sols. (Mar. 15, 2018) (last visited Jan. 18, 2022), https://axioncyber.com/data-breach/how-data-breaches-affect-children/.

35. The FBI's Internet Crime Complaint (IC3) 2019 estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone. The same report identified "rapid reporting" as a tool to help law enforcement stop fraudulent transactions and mitigate losses.

36. Defendant did not rapidly, or even reasonably, report to Plaintiffs and the Class that their Sensitive Information had been exposed or stolen. Instead, Defendant waited over four weeks after identifying the Data Breach before notifying the Class of the breach.

37. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[9]

38. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require:

(1) encrypting information stored on computer networks;

(2) retaining payment card information only as long as necessary;

(3) properly disposing of personal information that is no longer needed or can be disposed pursuant to relevant state and federal laws;

(4) limiting administrative access to business systems;

(5) using industry unapproved activity;

(6) monitoring activity on networks to uncover unapproved activity;

(7) verifying that privacy and security features function property;

[9] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited Jan. 18, 2022) http://www/ftc/gov/speeches/harbour/091207privacyroundtable.pdf.

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.[10]

39. The United States Government and the United States Cybersecurity & Infrastructure Security Agency recommend several similar and supplemental measures to prevent and detect cyber-attacks, including, but not limited to: implementing an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring firewalls, automating anti-virus and anti-malware programs, managing privileged accounts, configuring access controls, disabling remote desktop protocol, and updating and patching computers.

40. The FTC cautions businesses that failure to protect Sensitive Information and the resulting data breaches can destroy consumers' finances, credit history, and reputations, and can take time, money and patience to resolve the effect.[11] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures—like Defendant failed to do here—as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

D. The Healthcare Industry is Particularly Susceptible to Cyber Attacks.

41. A 2010 report focusing on healthcare data breaches found the "average total cost to resolve an identity theft related incident … came to about $20,000."[12] According to survey results and population extrapolations from the National Study on Medical Identity Theft report from the Ponemon Institute, nearly 50% of victims reported losing their healthcare coverage because of a

[10] *Start With Security, A Guide for Business,* FTC (last visited Jan. 18, 2022) https://www.ftc.gov/system/files/documents/plain-language/pdf0205.

[11] *See* Taking Charge, What to Do if Your Identity is Stolen, FTC, at 3 (2012) (last visited Jan. 19, 2022), www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

[12] *See* Elinor Mills, *Study: Medical identity theft is costly for victims,* CNET (March 3, 2010), (last visited Jan. 11, 2021), https://www.cnet.com/tech/services-and-software/study-medical-identity-theft-is-costly-for-victims/

data breach and nearly 30% reported an increase in their insurance premiums.[13] Several individuals were unable to fully resolve their identity theft crises. Healthcare data breaches are an epidemic and they are crippling the impacted individuals—millions of victims every year.[14]

42. According to an analysis of data breach incidents reported to the U.S. Department of Health and Human Services and the media, from 2015 and 2019, the number of healthcare related security incidents increased from 450 annual incidents to 572 annual incidents, likely a conservative estimate.[15]

43. According to the Verizon Data Breach Investigations Report, the health care industry, including hospitals and other providers, experienced 655 known data breaches, 472 of which had confirmed data disclosures in 2021.[16] For the tenth year in a row, the healthcare industry has seen the highest impact from cyber-attacks of any industry.[17]

44. The need for sufficiently robust cybersecurity, and the attractiveness of its data to third parties, was well known by Defendant.

45. As a healthcare data service engaged with numerous medical facilities servicing hundreds of thousands of patients, if not more, Defendant knew or should have known the

---

[13] *Id.*

[14] *Id.*

[15] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEALTHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=OVer%2041%20million%20patient%20records,close%20to%2021%20million%20records (last visited Jan.19, 2022).

[16] Verizon, 2021 Data Breach Investigations Report: Healthcare NAICS 62 (2021) (last visited Jan. 19, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/healthcare-data-breaches-security/.

[17] *Five worthy reads: The never-ending love story between cyberattacks and healthcare,* ManageEngine, https://blogs.manageengine.com/corporate/manageengine/2021/08/06/the-never-ending-love-story-between-cyberattacks-and-healthcare.html#:~:text=According%20to%20Infosec%20Institute%2C%20credit,is%20%24158%20per%20stolen%20record.

importance of protecting the Sensitive Information entrusted to it. Defendant also knew or should have known of the foreseeable, and catastrophic consequences if its systems were breached. These consequences include substantial costs to Plaintiffs and the Class because of the Data Breach. Despite this, Defendant failed to take reasonable data security measures to prevent or mitigate losses from cyberattacks.

E. Plaintiffs' and the Class's Sensitive Information is Valuable.

46. Unlike financial information, such as credit card and bank account numbers, the Sensitive Information exfiltrated in the Data Breach cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or her life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable to hackers.[18]

47. Birth dates, Social Security numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on an ongoing basis rather than exploiting just one account until it's canceled.[19] For that reason, Cybercriminals on the dark web are able to sell Social Security numbers for large profits. For example, an infant's social security number sells for as much as $300 per number.[20] Those numbers are often then used for fraudulent tax returns.[21]

---

[18] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters, https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited Jan. 18, 2022).

[19] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[20] *Id.*

[21] *Id.*

48. Consumers place a considerable value on their Sensitive Information and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth between $30.49 and $44.62.[22] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

49. Defendant's Data Breach exposed a variety of Sensitive Information, including dates of birth and Social Security numbers.

50. The Social Security Administration ("SSA") warns that a stolen Social Security number can lead to identity theft and fraud: "Identity thieves can use your number and your credit to apply for more credit in your name."[23] If the identity thief applies for credit and does not pay the bill, it will damage victims' credit and cause a series of other related problems.

51. Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

52. PHI, also at issue here, is likely even more valuable than Social Security numbers and just as capable of being misused. The Federal Bureau of Investigation ("FBI") has found

---

[22] 11-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore,* at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Jan. 19, 2022).

[23] Social Security Administration, *Identity Theft and Your Social Security Number*, (last visited Jan. 19, 2022), https://www.ssa.gov/pubs/EN-05-10064.pdf.

instances of PHI selling for fifty times the price of stolen Social Security numbers or credit card numbers.[24]

53. Other reports found that PHI is ten times more valuable on the black market than credit card information.[25] This is because one's personal health history, including prior illness, surgeries, diagnoses, mental health, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, social security numbers. Credit card information and PII sell for $1-2 on the black market, but PHI can sell for as much as $363 according to the Infosec Institute.[26]

54. Cybercriminals recognize and exploit the value of Sensitive Information. The value of Sensitive Information is the foundation to the cyberhacker business model.

55. Because the Sensitive Information exposed in the Defendant's Data Breach is permanent data, there may be a gap of time between when it was stolen and when it will be used. The damage may continue for years. Plaintiffs and the Class now face years of monitoring their financial and personal records with a high degree of scrutiny. The Class has incurred and will incur this damage in additional to any fraudulent use of their Sensitive Information.

F. Defendant's Conduct Violates HIPAA.

56. Defendant is a Covered Entities under HIPAA. As a regular and ordinary part of its business, Defendant collects and maintains the Sensitive Information of its clients' patients.

---

[24] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-healthcare-cyber-intrusions/ (last visited Jan. 18, 2022).

[25] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[26] *Hackers Selling Healthcare Data in the Black Market*, INFOSEC, https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 18, 2022).

Defendant is therefore required under state and federal law to confidentiality of the Sensitive Information that it collects and maintains, and is further required to implement and maintain sufficient safeguards to protect that Sensitive Information from third parties.

57. Plaintiffs and the Class entrusted Defendant with their Sensitive Information, and by collecting and deriving a benefit from Plaintiffs' and the Class Members' Sensitive Information, Defendant assumed legal and equitable duties and know or should have known that it was responsible for protecting the Sensitive Information from unauthorized disclosure.

58. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), individuals' health information must be:

> properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.[27]

59. HIPAA is a "federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[28] The rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.[29]

60. HIPAA defines sensitive patient personal and health information as: (1) Name; (2) Home and work addresses; (3) Home and work phone numbers; (4) Personal and professional email addresses; (5) Medical records; (6) Prescriptions; (7) Health insurance information; (8)

---

[27] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Jan. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[28] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Jan. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/security/index.html.

[29] *Id.*

Billing information; (9) Social Security number; (10) Spouse and children's information; and/or (11) Emergency contact information.[30]

61. To ensure protection of this private and sensitive information, HIPAA mandates standards for handling PHI—the very data Defendant failed to protect. The Data Breach resulted from Defendant's failure to comply with several of these standards:

a. Violation of 45 C.F.R. § 164.306(a)(1): failing to ensure the confidentiality and integrity of electronic protected health information that Defendant created, received, maintained, and transmitted;

b. Violation of 45 C.F.R. § 164.312(a)(1): Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;

c. Violation of 45 C.F.R. § 164.308(a)(1): Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

d. Violation of 45 C.F.R. § 164.308(a)(6)(ii): Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity;

e. Violation of 45 C.F.R. §164.306(a)(2): Failing to protect against any reasonably–anticipated threats or hazards to the security or integrity of electronic protected health information;

f. Violation of 45 C.F.R. §164.306(a)(3): Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information;

g. Violation of 45 C.F.R. §164.306(a)(94): Failing to ensure compliance with HIPAA security standard rules by its workforce;

h. Violation of 45 C.F.R. §164.502, et seq: Impermissibly and improperly using and disclosing protected health information that is, and remains, accessible to unauthorized persons; and

i. Violation of 45 C.F.R. §164.530(c): Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information.

[30] *Id.*

62. Despite Defendant's failure to reasonably protect Plaintiffs' and the Class's Sensitive Information, it has not offered any compensation or adequate remedy considering the significant and long-term risk Plaintiffs and the Class face.

G. Plaintiff's Experiences

a. Plaintiff Rita May's Experience

63. Plaintiff Rita May used Apria's services and devices for a medical condition.

64. As a condition to receiving services from Apria, Plaintiff provided her Sensitive Information to Apria which was then entered into Apria's database and maintained by Apria.

65. Plaintiff greatly values her privacy and Sensitive Information, especially when receiving health or health insurance services. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of her Sensitive Information.

66. Plaintiff received a Notice of Data Breach letter dated June 6, 2023, from Apria informing her that unauthorized actors gained access to files on Apria's computer network that contained her patient account number, address, dates of services, email address, name, and telephone number.

67. Plaintiff only allowed Apria to maintain, store, and use her Sensitive Information because she believed that Apria would use reasonable security measures in compliance with applicable law to protect her Sensitive Information. As a result, Plaintiff's Sensitive Information was within the possession and control of Apria at the time of the Data Breach.

68. Plaintiff is very careful about sharing her Sensitive Information. Plaintiff stores any documents containing her Sensitive Information in a safe and secure location. She has never knowingly transmitted unencrypted Sensitive Information over the internet or any other unsecured

source. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

69. As a result of the Data Breach, and at the direction of Apria's Notice of Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, monitoring her credit and reviewing her financial accounts for any indication of fraudulent activity. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

70. Plaintiff suffered actual injury from having her Sensitive Information compromised as a result of the Data Breach, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of her Sensitive Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of the benefit of her bargain with Apria; (v) the disclosure of her Sensitive Information; and (vi) the continued and certainly increased risk to her Sensitive Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Apria's possession and subject to further unauthorized disclosures so long as Apria fails to undertake appropriate and adequate measures to protect the Sensitive Information.

71. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Apria has not been forthright with information about the Data Breach.

72. Plaintiff plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

73. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains in Apria's possession, is protected and safeguarded from future breaches.

b. Plaintiff Tammie Creek's Experience

74. Plaintiff Tammie Creek used Apria's services and devices for a medical condition.

75. As a condition to receiving services from Apria, Plaintiff provided her Sensitive Information to Apria which was then entered into Apria's database and maintained by Apria.

76. Plaintiff greatly values her privacy and Sensitive Information, especially when receiving health or health insurance services. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of her Sensitive Information.

77. Plaintiff received a Notice of Data Breach letter dated June 6, 2023, from Apria informing her that unauthorized actors gained access to files on Apria's computer network that contained her date of birth, device descriptions, health insurance policy number or subscriber number, medical history, patient account number, name, telephone number, and Social Security number.

78. Plaintiff only allowed Apria to maintain, store, and use her Sensitive Information because she believed that Apria would use reasonable security measures in compliance with applicable law to protect her Sensitive Information. As a result, Plaintiff's Sensitive Information was within the possession and control of Apria at the time of the Data Breach.

79. Plaintiff is very careful about sharing her Sensitive Information. Plaintiff stores any documents containing her Sensitive Information in a safe and secure location. She has never knowingly transmitted unencrypted Sensitive Information over the internet or any other unsecured source. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

80. As a result of the Data Breach, and at the direction of Apria's Notice of Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, monitoring her credit and reviewing her financial accounts for any indication of fraudulent activity. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

81. Plaintiff suffered actual injury from having her Sensitive Information compromised as a result of the Data Breach, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of her Sensitive Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of the benefit of her bargain with Apria; (v) the disclosure of her Sensitive Information; and (vi) the continued and certainly increased risk to her Sensitive Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Apria's possession and subject to further unauthorized disclosures so long as Apria fails to undertake appropriate and adequate measures to protect the Sensitive Information.

82. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Apria has not been forthright with information about the Data Breach.

83. Plaintiff plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

84. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains in Apria's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

85. Plaintiffs bring this action against Defendant on behalf of themselves and all other persons similarly situated ("the Class") pursuant to Fed. R. Civ. P. 23.

86. Plaintiffs propose the following Class definition:

All persons who were impacted by Defendant's Data Breach.

87. Excluded from the Class is Defendant; its officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest in, is a parent or subsidiary of, or which is otherwise controlled by Defendant; and Defendant's affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assignees. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

88. Plaintiffs reserve the right to modify and/or amend the Class definition, including but not limited to creating additional subclasses, as necessary.

89. All members of the proposed Class are readily identifiable through Defendant's records.

90. **Numerosity.** The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiffs are informed and believe that the proposed Class includes at least 3 million people. The precise number of Class members is unknown to Plaintiffs but may be ascertained from Defendant's records.

91. **Commonality and Predominance.** This action involves common questions of law and fact to the Plaintiffs and Class members, which predominate over any questions only affecting individual Class members. These common legal and factual questions include, without limitation:

a. Whether Defendant owed Plaintiffs and the other Class members a duty to adequately protect their Sensitive Information;

b. Whether Defendant owed Plaintiffs and the other Class members a duty to implement reasonable data security measures due to the foreseeability of a data breach;

c. Whether Defendant owed Plaintiffs and the other Class members a duty to implement reasonable data security measures because Defendant accepted, stored, and maintained highly sensitive information concerning Plaintiffs and the Class;

d. Whether Defendant knew or should have known of the risk of a data breach;

e. Whether Defendant breached its duty to protect the PII and PHI of Plaintiffs and other Class members;

f. Whether Defendant knew or should have known about the inadequacies of its data protection, storage, and security;

g. Whether Defendant failed to use reasonable care and reasonable methods to safeguard and protect Plaintiffs' and the Class's Sensitive Information from unauthorized theft, release, and disclosure;

h. Whether proper data security measures, policies, procedures and protocols were in enacted within Defendant's offices and computer systems to safeguard and protect Plaintiffs' and the Class's Sensitive Information from unauthorized theft, release or disclosure;

i. Whether Defendant's conduct was the proximate cause of Plaintiffs' and the Class's injuries;

j. Whether Plaintiffs and the Class suffered ascertainable and cognizable injuries as a result of Defendant's misconduct;

k. Whether Plaintiffs and the Class are entitled to recover damages; and

l. Whether Plaintiffs and the Class are entitled to other appropriate remedies including injunctive relief.

92. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiffs on behalf of themselves and the Class. Individual questions, if any, are slight by comparison in both quality and quantity to the common questions that control this action.

93. **Typicality.** Plaintiffs' claims are typical of those of other Class members because Plaintiffs' PHI and PII, like that of every other Class member, was misused and improperly disclosed by Defendant. Defendant's misconduct impacted all Class members in a similar manner.

94. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interest of the members of the Class, and has retained counsel experienced in complex consumer class action litigation and intend to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class.

95. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered

by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court.

CLAIMS

COUNT I
Negligence
(On behalf of Plaintiffs and the Class)

96. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

97. Defendant collected, maintained, and stored Plaintiffs' and the Class's Sensitive Information for the purpose of facilitating medical treatment to Plaintiffs and the Class.

98. Plaintiffs and the Class are a well-defined, foreseeable, and probable group of individuals that Defendant was aware, or should have been aware, could be injured by inadequate data security measures. The nature of Defendant's business requires patients to disclose to it Sensitive Information to receive adequate care, including, but not limited to, medical histories, dates of birth, social security numbers, addresses, phone numbers, and medical insurance information. Defendant uses, handles, gathers, and stores the Sensitive Information of Plaintiffs and the Class and, additionally, solicits and stores records containing Plaintiffs' and the Class's Sensitive Information.

99. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. Defendant knew or

should have known that its repository of a host of Sensitive Information for hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, Defendant had a duty to reasonably safeguard the Sensitive Information by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiffs and the Class of inadequate data security created a duty to act reasonably and safeguard the Sensitive Information.

100. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in safeguarding and protecting their Sensitive Information in its possession from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

101. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiffs' and the Class's Sensitive Information was adequately protected and secured. Defendant further had a duty to implement processes that would detect a breach of their security system in a timely manner.

102. Defendant also had a duty to timely disclose to Plaintiffs and the Class that their Sensitive Information had been or was reasonably believed to have been compromised. Timely disclosure is necessary so that, among other things, Plaintiffs and the Class may take appropriate measures to begin monitoring their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts and take all other appropriate precautions, including those recommended by Defendant.

103. Defendant also should have known that, given the Sensitive Information it held, Plaintiffs and the Class would be harmed should it suffer a Data Breach. Defendant knew or should have known that their systems and technologies for processing and securing Plaintiffs' and the Class's Sensitive Information had security vulnerabilities susceptible to cyber-attacks.

104. Despite that knowledge, Defendant implemented unreasonable data security measures that allowed cybercriminals to successfully breach Defendant's network and data environments, reside there undetected for a significant period of time, and access or steal a host of personal and healthcare information on millions of Defendant's patients.

105. Defendant, through its actions and/or omissions, failed to provide reasonable security for the data in its possession.

106. Defendant breached is duty to Plaintiffs and the Class by failing to adopt, implement, and maintain reasonable security measures to safeguard their Sensitive Information, allowing unauthorized access to Plaintiffs' and the Class's Sensitive Information, and failing to recognize the Data Breach in a timely manner. Defendant further failed to comply with industry regulations and exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class's Sensitive Information.

107. But for Defendant's wrongful and negligent breach of its duties, Plaintiffs' and the Class's Sensitive Information would not have been accessed and exfiltrated by unauthorized persons, and they would not face a risk of harm of identity theft, fraud, or other similar harms.

108. Additionally, Defendant failed to reasonably notify Plaintiffs of the Data Breach. Defendant waited over four weeks after discovering the Data Breach — including two weeks while the third party still had access to Defendant's systems after Defendant was aware of suspicious activity — to inform Plaintiffs that their information was accessed. The unreasonable delay in notifying Plaintiffs and the Class of the breach robbed them of the opportunity to take measures to protect against the misuse of their information and to monitor their accounts.

109. As a result of Defendant's negligence, Plaintiffs and the Class suffered damages including, but not limited to, ongoing and imminent threat of identity theft crimes; out-of-pocket

expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Defendant's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; decreased credit scores and ratings; and irrecoverable financial losses due to fraud.

COUNT II
Negligence *Per Se*
(On behalf of Plaintiffs and the Class)

110. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

111. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair ... practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

112. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's PHI and PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

113. To provide its health records and management services, Defendant collected, maintained, and stored Plaintiffs' and the Class's Sensitive Information.

114. Additionally, as a vendor serving covered entities under HIPAA, Defendant is covered by HIPAA, 45 C.F.R. § 160.102, and is therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

115. HIPAA, 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information."

116. Per 45 C.F.R. § 164.306, HIPAA "standards, requirements and implementation specifications" apply to covered entities, such as Defendant. HIPAA standards are mandatory.

117. HIPAA requires Defendant to "ensure the confidentiality, integrity, and availability of all electronic protected health information" it receives and to protect against any "reasonably anticipated threats or hazards to the security or integrity" of the Sensitive Information. 45 C.F.R. § 164.306.

118. Defendant violated HIPAA by failing to adhere to and meet the requirements of 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

119. Defendant violated HIPAA by failing to use reasonable measures to protect the Sensitive Information of Plaintiffs and the Class. Defendant's conduct was especially unreasonable given the nature of the Sensitive Information and the number of patients it serves, some of which are minors or patients who live below the federal poverty level, who may not have the means to expend significant amounts of time and money to fully mitigate the fallout of the Data Breach.

120. Defendant's violation of Section 5 of the FTC Act and HIPAA both separately and individually constitute negligence *per se*.

121. Plaintiffs and the Class are within the group of individuals the FTC Act and HIPAA were designed to protect and the harm to these individuals is a result of the Data Breach. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses

which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the proposed Class.

122. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class members suffered and continue to suffer injuries and are entitled to damages in an amount to be proven at trial.

123. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have been injured as described herein and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of an Implied Contract
(On Behalf of Plaintiffs and the Class)

124. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

125. Defendant offered to facilitate the provision of medical goods and services to Plaintiffs and members of the Class in exchange for payment.

126. Defendant also required Plaintiffs and the members of the Class to provide Defendant with their Sensitive Information, through their medical providers, in order to receive goods and services.

127. In turn, and through the Privacy Policy, Defendant agreed it would not disclose the patients' Sensitive Information to unauthorized persons. Defendant also promised to maintain safeguards to protect the patients' Sensitive Information.

128. Plaintiffs and the members of the Class accepted Defendant's offer by providing Sensitive Information, directly or indirectly, to Defendant in exchange for receiving Defendant's goods and services and then by paying for and receiving the same.

129. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and members of the Class with prompt and adequate notice of any and all unauthorized access and/or theft of their Sensitive Information.

130. Plaintiffs and the members of the Class would not have entrusted their Sensitive Information to Defendant in the absence of such agreement with Defendant.

131. Defendant materially breached the contract(s) it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breach the implied contracts with Plaintiffs and members of the Class by:

a. Failing to properly safeguard and protect Plaintiffs' and members of the Class's Sensitive Information;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

c. Failing to ensure the confidentiality and integrity of electronic Sensitive Information that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

132. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendant's material breaches of the implied agreement.

133. Plaintiffs and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of the Defendant.

134. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in

connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit – not merely the letter – of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

135. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

136. Defendant failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

137. In these and other ways, Defendant violated its duty of good faith and fair dealing.

138. Plaintiffs and members of the Class have sustained damages as a result of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

PRAYER FOR RELIEF

139. WHEREFORE, Plaintiffs respectfully pray for judgment in their favor as follows:

a. Certification the Class pursuant to the provisions of Fed. R. Civ. P. 23and an order that notice be provided to all Class Members;

b. Designation of Plaintiffs as representatives of the Class and the undersigned counsel, Zimmerman Reed LLP, as Class Counsel;

c. An award of damages in an amount to be determined at trial or by this Court;

d. An order for injunctive relief, enjoining Defendant from engaging in the wrongful and unlawful acts described herein;

e. An award of statutory interest and penalties;

f. An award of costs and attorneys' fees; and

g. Such other relief the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

140. Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: June 20, 2023

Respectfully submitted,

/s/ Tyler B. Ewigleben

JOHNSON FIRM
Tyler B. Ewigleben
Christopher D. Jennings*
Winston Hudson*
Laura Edmondson*
THE JOHNSON FIRM
610 President Clinton Ave., Suite 300
Little Rock, AR 72201
Tel: (501) 372-1300
chris@yourattorney.com
tyler@yourattorney.com
winston@yourattorney.com
ledmondson@yourattorney.com

Brian C. Gudmundson*
Rachel K. Tack*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
rachel.tack@zimmreed.com

Attorneys for Plaintiffs and the Proposed Class
*To be admitted *pro hac vice*